R E P U B L I Q U E F R A N C A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

FR 00/483
EJU

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 17 MARS 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA REGLE 17.1.a) OU b)

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 26 FEV 1999
N° D'ENREGISTREMENT NATIONAL 9902474
DÉPARTEMENT DE DÉPÔT 75 INPI PARIS B
DATE DE DÉPÔT 26 FEV. 1999

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

SCHLUMBERGER SYSTEMES
Test & Transactions
50 Av. Jean Jaurès - B.P 620-04
92542 MONTROUGE Cédex
A l'attention de Anne DANG TRAN

n°du pouvoir permanent PG07391 | références du correspondant 76-0557 | téléphone 01 47 46 72 14

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ☐ demande initiale
☐ certificat d'utilité ☐ transformation d'une demande de brevet européen ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☒ non

Titre de l'invention (200 caractères maximum)

DISPOSITIF ET PROCEDE DE SECURISATION D'UN MEDIA DE STOCKAGE DE DONNEES

3 DEMANDEUR (S) n° SIREN 5 6 2 1 1 3 5 3 0 code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

SCHLUMBERGER SYSTEMES

Forme juridique

Société Anonyme

Nationalité (s)

Française

Adresse (s) complète (s)

50, avenue Jean Jaurès
92120 MONTROUGE

Pays

France

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande
SANS			

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(nom et qualité du signataire - n° d'inscription)

Anne DANG TRAN
Mandataire
(PG07391)

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS
26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

76-0557

N° D'ENREGISTREMENT NATIONAL
9902474

TITRE DE L'INVENTION :

DISPOSITIF ET PROCEDE DE SECURISATION D'UN MEDIA DE STOCKAGE DE DONNEES

LE(S) SOUSSIGNÉ(S)

Anne DANG TRAN
SCHLUMBERGER SYSTEMES
Test & Transactions
50, avenue Jean Jaurès - BP 620-04
92542 MONTROUGE Cédex

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

FAUSSE Arnaud
11 bis rue de Maubeuge
75009 PARIS
FRANCE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Le 26 février 1999

Anne DANG TRAN
(PG 07391)

DISPOSITIF ET PROCEDE DE SECURISATION D'UN MEDIA DE STOCKAGE DE DONNEES

La présente invention concerne un dispositif de sécurisation d'un média de stockage de données. Elle concerne également un procédé de sécurisation d'un tel dispositif.

L'invention trouve une application particulièrement avantageuse dans des domaines tels que les domaines de l'informatique, des jeux, de l'audiovisuel.... Les médias de stockage de données comprennent des données destinées à être exploitées généralement sur un terminal tel qu'un ordinateur ou un moniteur de télévision. Lesdites données sont des informations de type texte, des images, du son ou encore des logiciels.

De nombreuses copies frauduleuses des données contenues dans lesdits médias sont effectuées au moyen de logiciels accessibles à tous. Ces logiciels permettent de dupliquer des données d'un média en dépit des droits d'auteurs qui protègent généralement lesdites données. Un dispositif connu de l'état de l'art propose d'utiliser un boîtier de sécurité pour empêcher les copies pirates des données contenues dans un média. Le boîtier qui contient un circuit électronique d'identification est relié par exemple à un ordinateur dans lequel est introduit ledit média. Ledit dispositif divulgue la présence d'un programme dans le média permettant d'identifier le boîtier de sécurité par l'intermédiaire dudit circuit électronique. Le programme est chargé dans l'ordinateur puis il effectue l'identification. En cas d'absence du boîtier approprié, les données ne peuvent être lues, par suite, le média ne peut être utilisé. Le dispositif n'offre qu'une sécurité minimale dans la mesure où le programme de vérification peut être neutralisé sur l'ordinateur. Il n'existe alors plus aucune protection. De plus, généralement, un boîtier de sécurité est associé à un seul média. Par suite, la gestion de la

sécurité devient très onéreuse et compliquée puisqu'il faut un nouveau boîtier de sécurité pour tout nouveau média.

Aussi un problème technique à résoudre par l'objet de la présente invention est de proposer un dispositif de sécurisation d'un média de stockage de données, ainsi qu'un procédé de sécurisation d'un tel dispositif, qui permettent d'éviter les copies frauduleuses des données contenues dans lesdits médias tout en n'alourdissant pas l'utilisation desdits médias.

Une solution au problème technique posé se caractérise, selon un premier objet de la présente invention, en ce que ledit dispositif comporte, intégrés dans ledit média, d'une part, un objet portatif comportant une mémoire comprenant au moins une clef secrète unique audit média, et, d'autre part, des moyens d'échange de données, ladite clef permettant de décrypter des données dudit média, lesdits moyens d'échange permettant d'échanger lesdites données entre ledit objet portatif et ledit média.

Selon la présente invention, un procédé de sécurisation d'un média de stockage de données est remarquable en ce que le procédé comporte les étapes consistant à :

- on décrypte des données dudit média au moyen d'une clef secrète, unique audit média, contenue dans une mémoire d'un objet portatif intégré audit média,
- on échange les données dudit média entre ledit objet portatif et ledit média grâce à des moyens d'échange de données intégrés audit média.

Ainsi, comme on le verra en détail plus loin, le dispositif de l'invention permet de protéger des données du média en les cryptant et d'empêcher ainsi une lecture en clair des données. Une copie des données est inutilisable puisque lesdites données sont cryptées. Pour effectuer une lecture desdites données, ces dernières doivent être au

préalable décryptées au moyen d'une clef secrète contenue dans ledit objet, lequel est intégré dans le média de stockage de données. La clef secrète est unique à un média. Ainsi, une lecture en clair de données est uniquement possible à partir dudit média.

La description qui va suivre au regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est une vue de dessus d'un média de stockage comportant un dispositif de sécurisation conforme à l'invention.

La figure 2 est un schéma d'un objet portatif compris dans le dispositif de sécurisation de la figure 1.

La figure 3 est une vue de côté d'un lecteur de média, du média et du dispositif de sécurisation de la figure 1.

La figure 4 est un schéma logique du lecteur de média de la figure 3.

La figure 5 est un autre schéma logique du lecteur de média de la figure 3.

La figure 6 est une vue partielle en perspective du lecteur de média de la figure 3.

La figure 7 est une vue de dessus d'une première réalisation du dispositif de sécurisation de la figure 1.

La figure 8 est une vue de dessus d'une seconde réalisation du dispositif de sécurisation de la figure 1.

La figure 9 est une vue de dessus partielle du lecteur de média de la figure 3.

La figure 10 est un schéma de données provenant du média de la figure 1.

La figure 11 est un autre schéma de données provenant du média de la figure 1.

Sur la figure 1 est représenté un média 10 de stockage de données. Ledit média intègre un objet portatif 20 et des moyens d'échange de données. Le média 10 comporte trois zones principales. La zone périphérique 11 permet de stocker des données. Les deux autres zones sont des zones centrales. L'une est un trou 13 placé au centre du média et dans lequel un axe mécanique peut se glisser, ladite zone correspond ainsi à un axe de rotation. L'autre est une zone neutre 12 placée entre le trou 13 et la zone périphérique 11 et ne contenant aucune donnée. Ledit objet portatif 20 est intégré dans une zone centrale dudit média 10 qui est la zone neutre 12. Comme le montre la figure 2, l'objet portatif 20 comprend une mémoire 22 et un bloc de contacts 23 permettant d'établir des contacts électriques avec par exemple un terminal. La mémoire 22 comprend une clef K1 secrète. Cette clef est unique pour chaque média, c'est à dire qu'elle n'a pas de doublet, ni dans le média auquel elle appartient, ni dans d'autres médias. Ledit objet portatif 20 comprend un cryptoprocesseur 21.

Ledit média 10 est un disque optique. Un disque optique est un disque composé de pistes comportant des données. Lesdites données comprennent un logiciel d'application tels que par exemple un logiciel de jeu vidéo ou d'exploitation de bases de données.

La suite du présent exposé de l'invention a trait à l'exemple des CD-ROM. Néanmoins, il est bien entendu que l'invention s'applique de manière générale à tout autre disque optique.

Dans le cas d'un CD-ROM, les données d'une piste sont formatées suivant des standards tels que ceux appelés Livre Jaune et Livre Vert définis par Philips. Les standards définissent essentiellement deux modes de formatage de données. Suivant un premier mode appelé mode 1, la piste comporte des données utilisateurs, des données d'entête et des données de détection d'erreurs permettant d'avoir deux niveaux de détection d'erreurs. Suivant un deuxième mode appelé mode 2, la piste

comporte des données utilisateurs, des données d'entête et des données de détection d'erreurs permettant d'avoir un seul niveau de détection d'erreurs. Les données d'entête comprennent un numéro de piste et des indicateurs de début et fin de piste. Les données utilisateurs comprennent le logiciel d'application.

Le média 10 connaît trois grandes phases. Une phase de fabrication, une phase dite de gravure-personnalisation et une phase d'utilisation.

Lors de la phase de fabrication, on place le média 10 sur une machine de fraisage qui réalise un logement dans lequel on intègre l'objet portatif 20. Ledit objet est inséré et collé dans le logement. Cependant, le poids dudit objet portatif peut déséquilibrer ledit média 10. Afin d'éviter ce problème, on prévoit que ledit média 10 comporte des moyens E d'équilibrage permettant d'équilibrer ledit média en le replaçant son centre de gravité sur son axe de rotation. Un mode de réalisation non limitatif desdits moyens d'équilibrage se fera au moyen d'une masselotte d'équilibrage composée d'une rondelle de métal collée dans un fraisage effectué dans ledit média, ladite masselotte étant diamétralement opposée audit objet portatif 20 du média 10, comme le montre la figure 1. La phase de fabrication est terminée.

Lors de la phase de gravure-personnalisation, des données sont cryptées et inscrites dans le média 10. Le cryptage et l'inscription, appelée aussi gravage, se font au moyen d'une machine de gravage. On prévoit que ladite machine de gravage est composée essentiellement des éléments suivants :

- une sonde munie de contacts permettant un échange de données entre un ordinateur pilotant ladite machine et l'objet portatif 20 intégré du média 10,
- un cryptoprocesseur représentant un algorithme de cryptage, permettant de crypter des données à graver,

- un logiciel générateur de clefs secrètes,
- un logiciel de chargement de clefs secrètes dans l'objet portatif 20 du média 10.

La phase de gravure-personnalisation se déroule selon les étapes suivantes :

- on charge un média 10 vierge,
- on génère un jeu individuel de clefs secrètes uniques,
- on détermine les données à crypter,
- on crypte les données au moyen d'une clef K1 secrète unique,
- on inscrit lesdites données cryptées dans ledit média 10 ainsi que les données non cryptées,
- on charge le jeu individuel de clefs secrètes uniques dans l'objet portatif 20 du média 10.

La clef K1 secrète unique provient du jeu individuel de clefs généré. Ladite clef K1 est soit l'une des clefs du jeu de clefs, soit une combinaison de clefs dudit jeu. On peut choisir de crypter toutes les données du média ou seulement une partie. Une piste comporte des blocs de données de deux mille quarante huit octets. Les données sont cryptées par groupe de huit octets si on utilise un algorithme de cryptage tel que le DES. D'autres algorithmes symétriques de cryptage peuvent être utilisés. L'ensemble des données est gravé dans la zone périphérique 11 du média. Le gravage se fait par des procédés connus tels que les procédés de type magnéto-optique ou brûlage de colorant par laser.

Désormais, le média 10 peut être utilisé.

Lors de la phase d'utilisation, dans une première étape, on lit les données qui se trouvent dans le média 10. La lecture se fait au moyen d'un lecteur 30 de média. Comme le montrent les figures 3 et 4, le lecteur est composé essentiellement d'un plateau 35 dans lequel vient se loger le média 10, d'un moteur M permettant de faire tourner le

média 10, d'un axe 32 mécanique qui vient se glisser dans le trou 13 du média 10, de deux plaques 33 et 34, permettant de maintenir le média 10 stable lorsque le lecteur fonctionne, d'une tête 31 de lecture laser comportant notamment une diode laser et des photodétecteurs, la diode laser permettant d'obtenir un faisceau laser, d'une interface 36 de type standard IDE ou SCSI permettant de connecter ledit lecteur 30 à un ordinateur 40, et, d'une interface 37 cryptoprocesseur permettant un dialogue avec le cryptoprocesseur 21 de l'objet portatif 20. La plaque 34 est appelée poupée et est solidaire de l'axe 32.

La lecture se fait de manière optique avec le faisceau laser et est définie dans des standards appelés tel que le Livre Bleu édité par Philips. Elle se fait suivant un procédé qui s'appuie sur la détection de la réflexion d'un faisceau laser sur une piste tantôt réfléchissante tantôt absorbante définissant ainsi des données se présentant sous forme de lumière. Le faisceau laser est par la suite dirigé vers les photodétecteurs qui sont des transducteurs permettant une conversion de la lumière en signaux électriques. Lesdits signaux électriques sont traités à un premier niveau afin d'éliminer des erreurs de discordance lors d'une lecture de données. La piste est par suite reconstituée, puis un code correcteur de deuxième niveau est appliqué lorsque celle-ci est formatée avec le mode 1. Par la suite, ladite piste est envoyée à l'interface 36 dudit lecteur 30 de média.

Le média 10 ainsi que le lecteur 30 de média ne comportent aucune indication permettant de dissocier les données cryptées des données non cryptées d'une piste. Ceci permet d'éviter une fraude qui consisterait à copier les indications portant sur un mode de cryptage des données contenues dans le média 10.

Dans une deuxième étape, le lecteur 30 de média reconnaît si le média 10 est équipé d'un cryptoprocesseur. A cette fin, il envoie la piste lue, via son interface 37 cryptoprocesseur, au média 10. Dans le cas où

des données sont renvoyées par ledit média via un premier canal 361 de communication ouvert au préalable lors de la lecture dudit média 10, ledit canal étant compris dans l'interface 36, le lecteur 30 conclura à la présence d'un média 10 comportant un objet portatif 20 composé d'un cryptoprocesseur 21. Dans le cas contraire, aucune donnée n'est renvoyée, par conséquent, le média 10, ne contient aucun cryptoprocesseur et la lecture des données se fait sans décryptage.

Dans une troisième étape, dans le cas où le média 10 est équipé d'un cryptoprocesseur, comme le montre la figure 4, les données DATA lues sont envoyées à l'ordinateur 40 relié audit lecteur 30, via un deuxième canal 362 de communication ouvert au préalable lors de la lecture dudit média 10, ledit canal étant compris dans l'interface 36. Ces données sont appelées données brutes car elles ne subissent aucune modification. Dans le même temps, on envoie les données DATA lues au cryptoprocesseur 21. Selon un premier moyen de réalisation, on envoie lesdites données DATA, via l'interface 37 cryptoprocesseur.

Selon un deuxième moyen de réalisation, comme le montre la figure 5, on envoie, au cryptoprocesseur 21 de l'objet portatif 20, lesdites données DATA au moyen d'un bus 38 de liaison série universelle appelée USB, ledit bus étant intégré dans l'ordinateur 40. Par suite, un unique canal de communication compris dans l'interface 36 du lecteur 30 est nécessaire. Les données décryptées dans ledit cryptoprocesseur 21 sont, par la suite, renvoyées à l'ordinateur 40 via ce même bus 38.

On notera que ce mode de réalisation est utilisable également lors de la deuxième étape décrite précédemment.

Lors de l'envoi des données DATA lues audit cryptoprocesseur, on transfère les signaux électriques correspondants auxdites données, du lecteur 30 de média au média 10, et, du média 10 à l'objet portatif 20,

grâce aux moyens d'échange de données intégrés audit média et à des moyens d'échange intégrés au lecteur 30 de média.

Soit, les moyens d'échange de données intégrés audit média 10 sont avec contacts, soit, les moyens d'échange de données intégrés audit média 10 sont sans contacts.

Dans le cas de moyens d'échange de données sans contacts, selon un mode de réalisation non limitatif de l'invention, les moyens d'échange de données intégrés audit média 10 sont une antenne. Les moyens d'échange de données intégrés au lecteur 30 sont une seconde antenne. Dans ce cas, les données sont échangées par couplage inductif entre lesdites première et seconde antennes.

Dans le cas de moyens d'échange de données avec contacts, selon un premier mode de réalisation non limitatif de l'invention, comme le montre la figure 6, des premiers moyens IN_B, OUT_B, VCC_B et GRD_B d'échange sont intégrés au lecteur 30 de média au niveau de l'axe 32 et de la poupée 34, et, comme le montre la figure 7 et les moyens IN_A, OUT_A, VCC_A et GRD_A d'échange de données sont intégrés au média 10 au niveau d'une zone centrale qui est la zone neutre 12. Lorsque la poupée 34 est en contact avec le média 10, Les premiers moyens entrent en contact respectivement avec les deuxièmes moyens. Cela permet d'échanger des données entre ledit lecteur de média et ledit média. En outre, les deuxièmes moyens IN_A, OUT_A, VCC_A et GRD_A intégrés au média 10, sont reliés au bloc 23 de contacts de l'objet portatif 20 en des points de contact respectifs I, O, V et G. Lesdits deuxièmes moyens IN_A, OUT_A, VCC_A et GRD_A permettent également un échange de données entre ledit média 10 et ledit objet portatif 20. Ainsi, lesdits moyens d'échange de données, intégrés au média 10 et au lecteur 30, comprennent des moyens d'échange d'entrée IN_A, IN_B, des moyens d'échange de sortie OUT_A,

OUT_B, des moyens VCC_A, VCC_B d'alimentation et des moyens GRD_A, GRD_B de mise à la masse.

Les moyens d'échange d'entrée IN_A et IN_B permettent de transporter des données du lecteur de média via le média 10. Le point de contact I et le moyen d'entrée IN_A permettent de transmettre les données du média 10 vers l'objet portatif 20. Les moyens d'échange de sortie OUT_A et OUT_B permettent de transporter des données du média 10 via le lecteur 30 de média. Le point de contact O et le moyen de sortie OUT_A permettent de transmettre les données de l'objet portatif 20 vers le média 10. Les moyens VCC_A et VCC_B d'alimentation permettent d'alimenter en tension ledit objet 20 portatif et les moyens GRD_A et GRD_B de mise à la masse permettent une mise à la masse dudit objet portatif.

Selon un second mode de réalisation, les moyens d'échange d'entrée IN_A, IN_B et de sortie OUT_A, OUT_B de données peuvent être confondus et être ainsi des moyens d'échange bidirectionnels.

On notera que selon un autre mode de réalisation, les premiers moyens IN_B, OUT_B, VCC_B et GRD_B d'échange de données intégrés au lecteur 30 de média peuvent être intégrés au niveau de la plaque inférieure 33 du lecteur.

Pour permettre un transport efficace des signaux électriques, les moyens d'échanges de données précités intégrés audit média 10 sont composés d'un matériau permettant une bonne conductivité et évitant une trop grande oxydation desdits moyens. Ainsi, ils sont composés d'or. Lesdits moyens peuvent, par exemple, être des anneaux comme le montre la figure 7, des fils ou encore des arcs de cercles comme le montre la figure 8. Il en est de même avec les moyens d'échange de données intégrés au lecteur 30 de média. Préférentiellement, afin d'éviter la présence d'une boucle sensible au rayonnement électromagnétique et par suite d'éviter des parasites dus à ce

rayonnement, les moyens d'échanges de données intégrés audit média 10 sont des arcs de cercle formant un secteur circulaire d'angle BETA et les moyens d'échange de données du lecteur 30 sont des arcs de cercle espacés d'un angle ALPHA inférieur à l'angle BETA, comme le montre la figure 9. Les arcs de cercles du média 10 et du lecteur 30 sont de même largeur W et sont distants d'une même largeur L. On garantit ainsi un contact permanent entre les différents moyens d'échange de données.

Après que les signaux électriques correspondants aux données DATA lues sont transmis à l'objet portatif 20 grâce aux moyens d'échanges de données définis précédemment, les données DATA sont décryptées au moyen d'un cryptoprocesseur qui les décrypte au moyen de la clef K1 secrète unique contenue dans la mémoire 22 de l'objet 20 portatif. Grâce à ce système de clef unique intégrée dans un objet portatif, une copie des données du média 10 sur un deuxième média, comportant ou non un cryptoprocesseur, est inutilisable. Ledit cryptoprocesseur représente un algorithme inverse de celui qui a été utilisé pour crypter lesdites données. Ledit cryptoprocesseur est programmé ou câblé.

Selon un premier mode de réalisation non limitatif, ledit cryptoprocesseur est intégré audit objet portatif 20. Selon un deuxième mode de réalisation, le cryptoprocesseur est un cryptoprocesseur rattaché au lecteur 30 de média. Dans ce deuxième mode de réalisation, il faut envoyer la clef K1 secrète de l'objet portatif 20 dans le lecteur de façon temporaire, le temps de décrypter les données DATA lues. Il est clair que dans ce cas il n'est nul besoin d'envoyer les données DATA à l'objet portatif 20. Cependant, on préférera le premier mode de réalisation qui est beaucoup plus sécuritaire étant donné que la clef K1 secrète demeure dans l'objet portatif 20 et n'est pas sujette à des fraudes qui consisterait à espionner le lecteur 30 de média pour reconstituer ladite clef K1 secrète.

Dans le cryptoprocesseur, les données DATA sont décryptées systématiquement, qu'elles soient à l'origine cryptées ou non, puis, le cas échéant, renvoyées audit lecteur 30, et enfin, transmises à l'ordinateur 40, via le premier canal 361 de communication si l'interface 37 cryptoprocesseur est utilisé.

On charge, de manière alternative, dans une mémoire 41 de l'ordinateur 40, les données DATA dudit média 10, cryptées et non cryptées. Comme le montre la figure 10, les données, non cryptées B dites brutes et décryptées D, sont envoyées à l'ordinateur 40 par pistes ou blocs complets, ou octets. On notera que les données non cryptées à l'origine, mais décryptées via le cryptoprocesseur 21 ne sont pas utiles. Cependant, le fait que le lecteur 30 délivre systématiquement à l'ordinateur 40 les données brutes et décryptées permet de se prémunir d'une attaque qui consisterait, d'une part, à différencier les données cryptées et non cryptées, et, d'autre part, à trouver une manière de les utiliser, en se connectant tout simplement à la sortie du lecteur 30 de média.

Dans une quatrième étape, les données envoyées et chargées dans la mémoire 41 de l'ordinateur 40 sont utilisées de la manière suivante : lesdites données, qui comprennent le logiciel d'application du média 10, sont composées d'un couple de pistes ou blocs, une piste ou un bloc B1 dit brut et une piste ou un bloc D1 dit décrypté ayant pour même origine une piste ou un bloc O1 de données lues dans le média 10. La figure 10 montre un bloc B1 brut qui est composé, d'une part, de zones Ba de données non cryptées, appelées zones utiles, et, d'autre part, de zones Bb de données cryptées inutilisables. Le bloc D1 décrypté est composé de zones Db de données décryptées inutilisables et de zones Da, appelées également zones utiles, de données décryptées correspondant aux zones Bb de données cryptées du bloc B1 brut.

Le logiciel d'application comprend, d'une part, un programme d'autodémarrage reconnu par l'ordinateur, qui permet d'initialiser ledit logiciel, et, d'autre part, du code exécutable. Ledit code exécutable comprend un ensemble de liens permettant de relier différentes zones entre elles, de charger de nouvelles données en mémoire, de reconstituer une zone de données. Ledit programme d'autodémarrage est chargé initialement dans l'ordinateur 40.

Les zones utiles des différents blocs comportent généralement, d'une part, une partie du code exécutable, et, d'autre part, des données d'application utilisées par le logiciel d'application telles que par exemple des images, du texte, du son.

Comme le montre la figure 11, le bloc B1 brut comporte une première zone B1Z1 utile dont le code exécutable s'exécute et utilise les données d'application nécessaires à ladite exécution. A la fin de l'exécution dudit code, un premier lien B1L1 permet de se positionner sur une première zone D1Z1 utile du bloc D1 décrypté. Le code de ladite zone s'exécute. A la fin de l'exécution dudit code, un lien D1L1 de ladite zone D1Z1 permet de se positionner sur une deuxième zone B1Z2 utile du bloc B1 brut dont le code s'exécute et ainsi de suite. Lorsque la dernière zone utile du bloc B1 brut s'exécute, un lien permet de charger en mémoire 41 de l'ordinateur les blocs ou pistes de données dont le logiciel d'application a besoin. Ainsi un ou plusieurs autres couples de pistes ou de blocs, brut et décrypté, sont lus et chargés en mémoire 41.

On notera que selon le dispositif de sécurisation, comprenant un cryptoprocesseur, décrit précédemment, le lecteur 30 pourra comprendre un service de décryptage. On enverra ainsi des données de l'ordinateur 40 vers le cryptoprocesseur 21 du média 10 afin qu'elles soient décryptées. Ce service sera utile pour certaines architectures de sécurité dans lesquelles le logiciel d'application aurait à décrypter des parties de pistes durant l'exécution dudit logiciel.

REVENDICATIONS

1 - Dispositif de sécurisation d'un média (10) de stockage de données, caractérisé en ce que ledit dispositif comporte, intégrés dans ledit média, d'une part, un objet (20) portatif comportant une mémoire (22) comprenant au moins une clef (K1) secrète unique audit média, et, d'autre part, des moyens d'échange de données, ladite clef (K1) permettant de décrypter des données (DATA) dudit média, lesdits moyens d'échange (IN_A, OUT_A, VCC_A, GRD_A) permettant d'échanger lesdites données entre ledit objet portatif et ledit média.

2 - Dispositif selon la revendication 1, caractérisé en ce que ledit média est un disque optique.

3 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que ledit objet portatif est intégré dans une zone centrale dudit média (10).

4 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que les moyens (IN_A, OUT_A, VCC_A, GRD_A) d'échange de données sont intégrés au média (10) au niveau d'une zone centrale.

5 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que ledit média (10) comporte des moyens (E) d'équilibrage permettant d'équilibrer ledit média.

6 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que les moyens d'échange de données intégrés audit média 10 sont avec contacts.

7 - Dispositif selon l'une des revendications 1 à 5, caractérisé en ce que les moyens d'échange de données intégrés audit média 10 sont sans contacts.

8 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que les données (DATA) sont décryptées au moyen d'un cryptoprocesseur.

9 - Dispositif selon la revendication 8, caractérisé en ce que ledit cryptoprocesseur est programmé ou câblé.

10 - Dispositif selon la revendication 8, caractérisé en ce que ledit cryptoprocesseur est intégré audit objet portatif (20).

11 - Procédé de sécurisation d'un média (10) de stockage de données, caractérisé en ce que le procédé comporte les étapes selon lesquelles :

- on décrypte des données (DATA) dudit média (10) au moyen d'une clef (K1) secrète, unique audit média, contenue dans une mémoire (22) d'un objet (20) portatif intégré audit média,
- on échange les données (DATA) dudit média (10) entre ledit objet portatif (20) et ledit média grâce à des moyens (IN_A, OUT_A, VCC_A, GRD_A) d'échange de données intégrés audit média.

12 - Procédé selon la revendication 11, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- on crypte des données au moyen d'une clef (K1) secrète unique,
- on inscrit lesdites données cryptées dans ledit média (10).

13 - Procédé selon l'une des revendications 11 ou 12, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- on charge, de manière alternative, dans une mémoire (41) d'un ordinateur (40), les données (DATA) dudit média (10), cryptées et non cryptées.

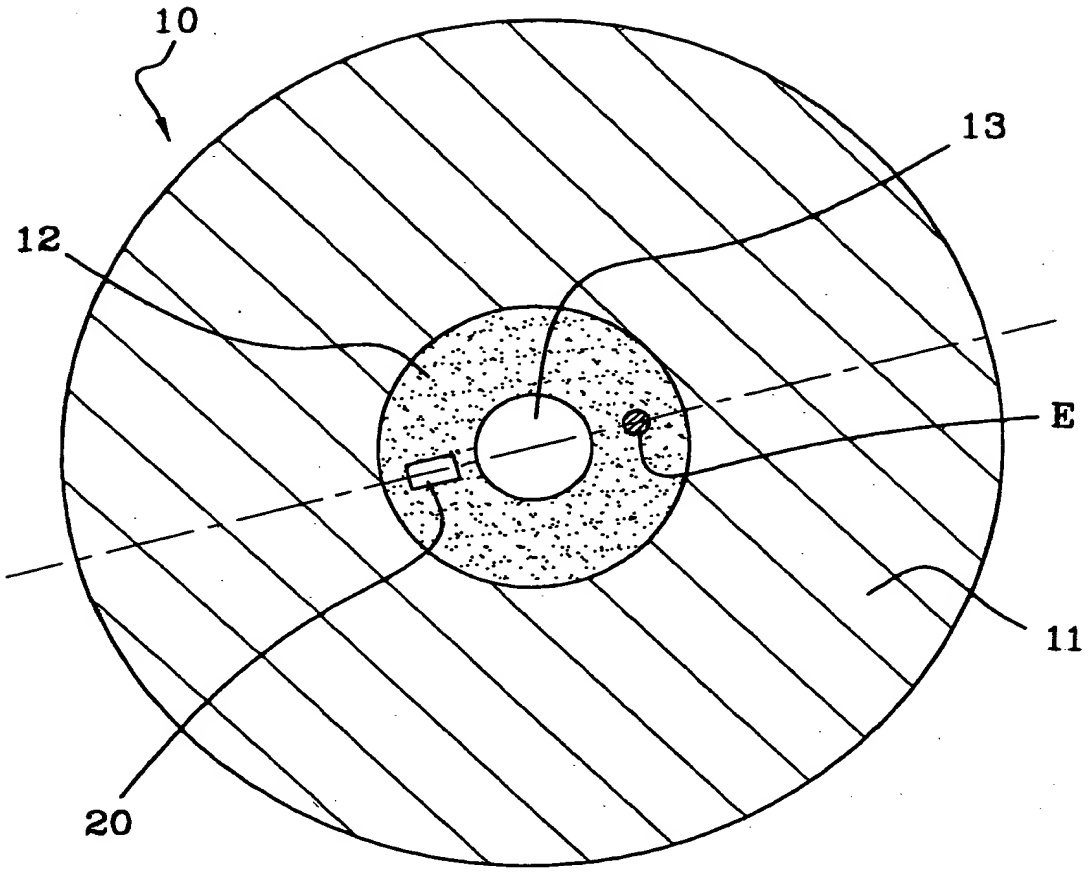

FIG.1

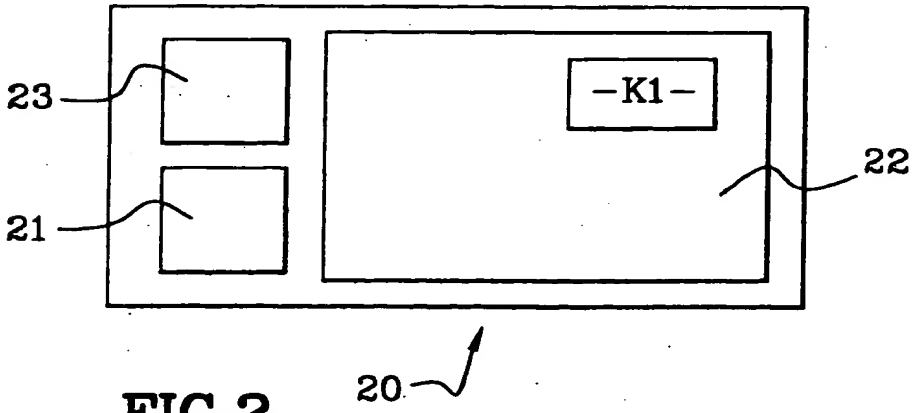

FIG.2

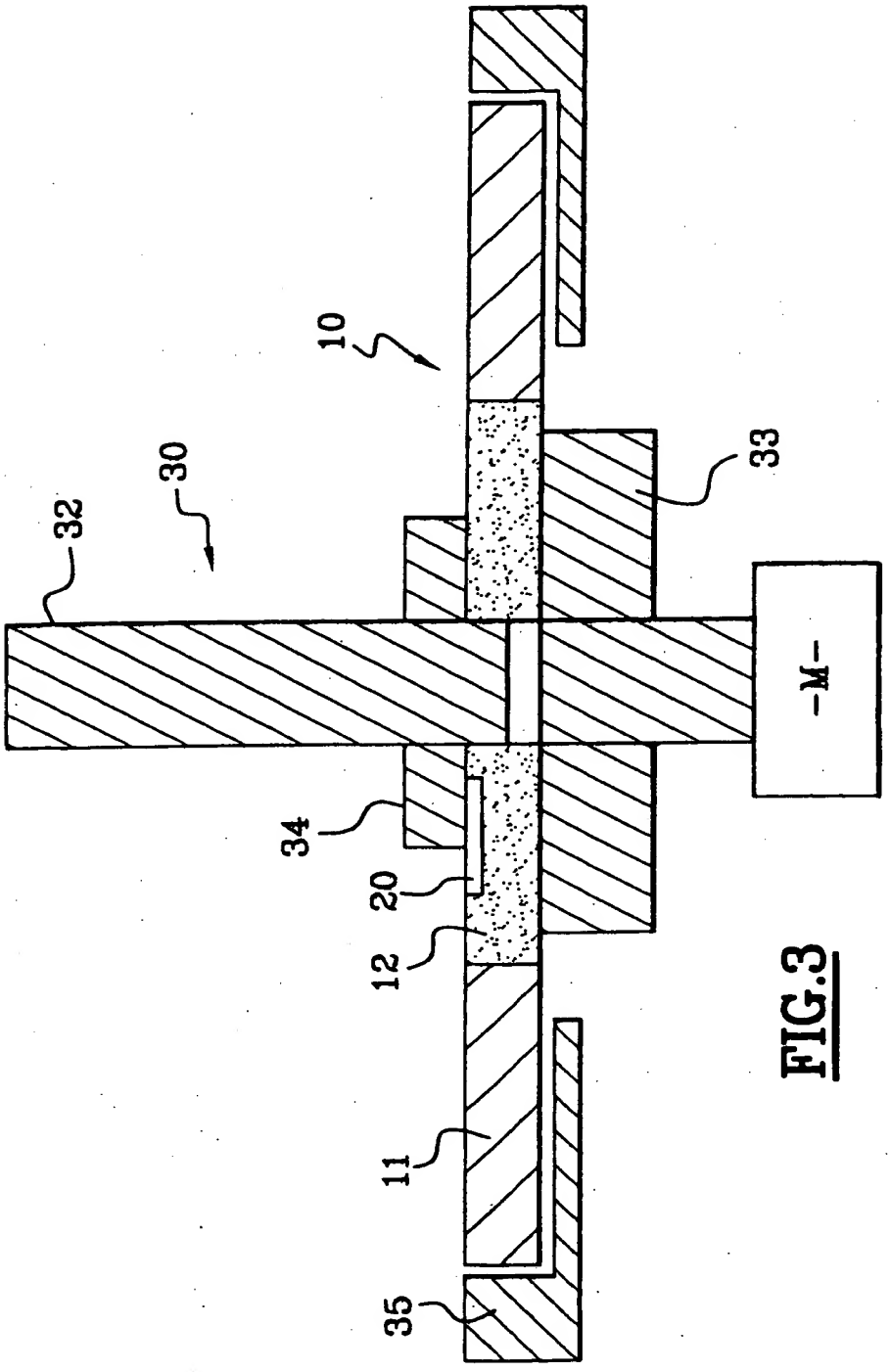

FIG.3

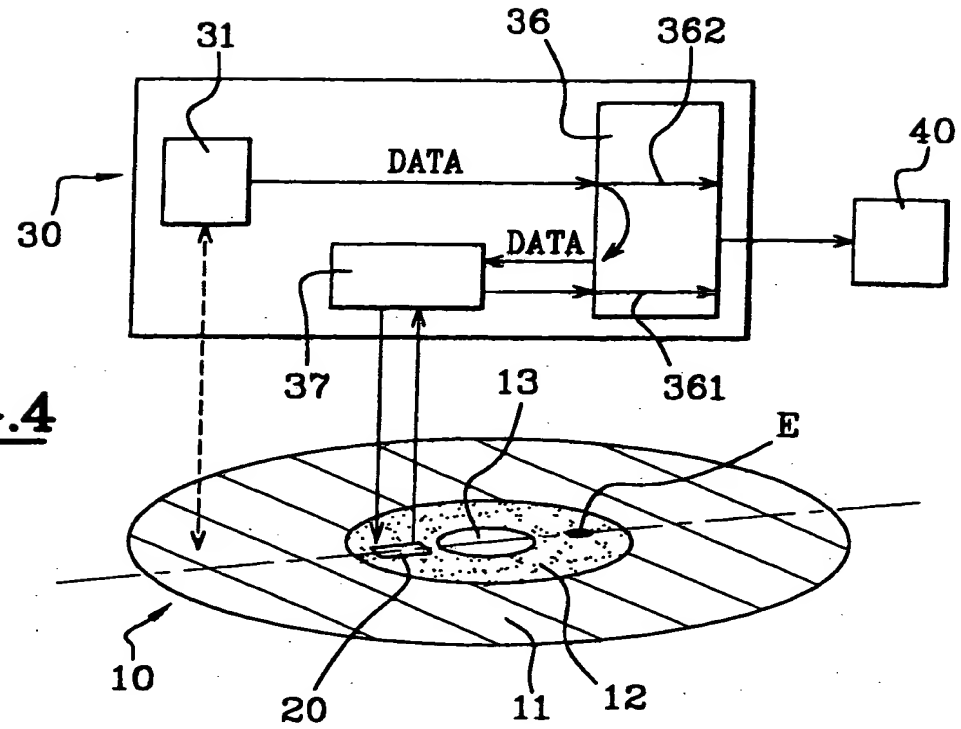
31
36
362
40
DATA
30
DATA
37
361
13
E
10
20
11
12

FIG.4

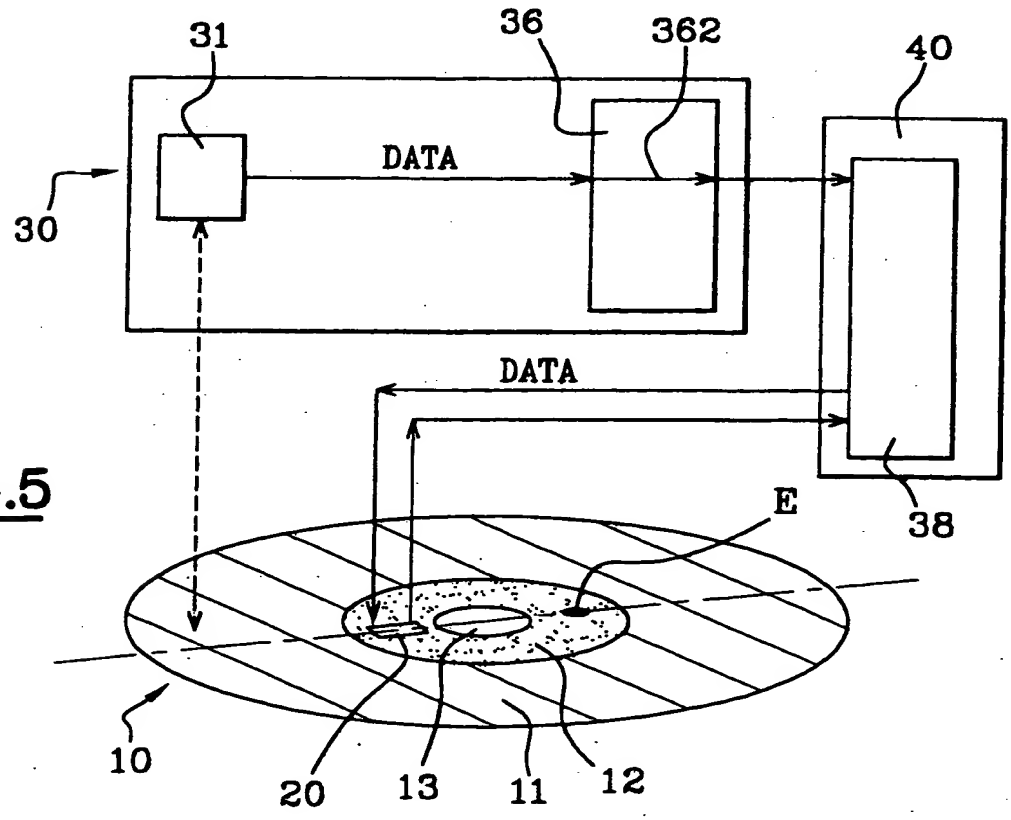
31
36
362
40
DATA
30
DATA
E
38
10
20
13
11
12

FIG.5

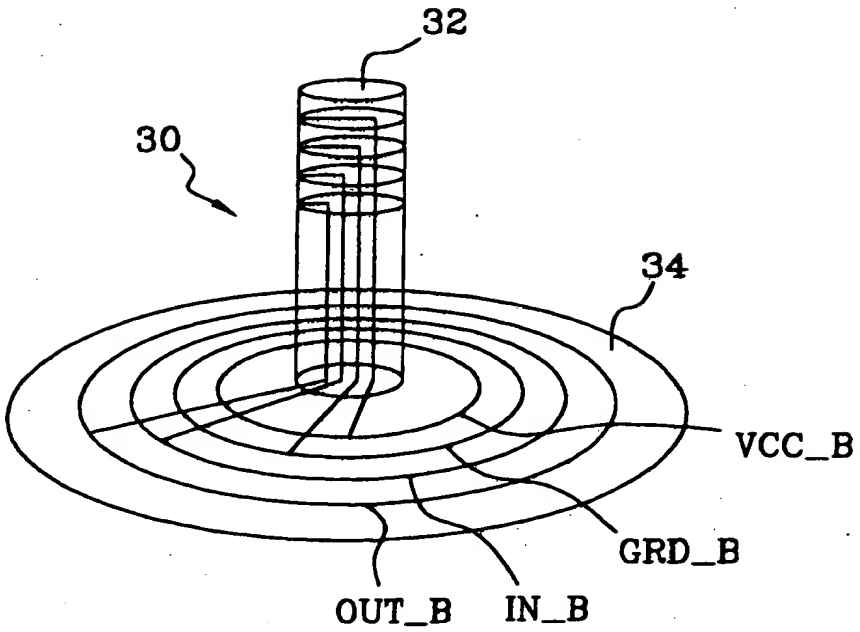
32
30
34
VCC_B
GRD_B
OUT_B
IN_B

FIG.6

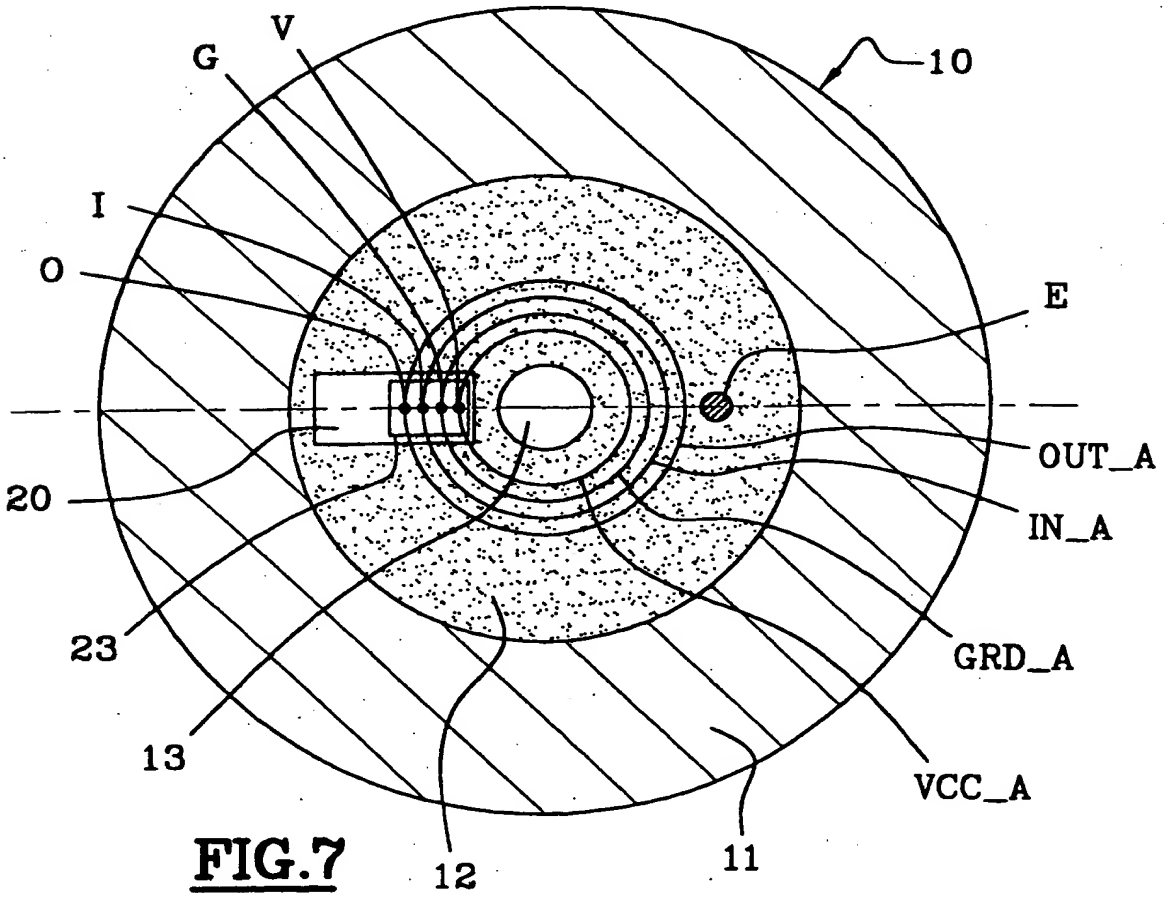
V
G
10
I
O
E
OUT_A
20
IN_A
23
GRD_A
13
VCC_A
12
11

FIG.7

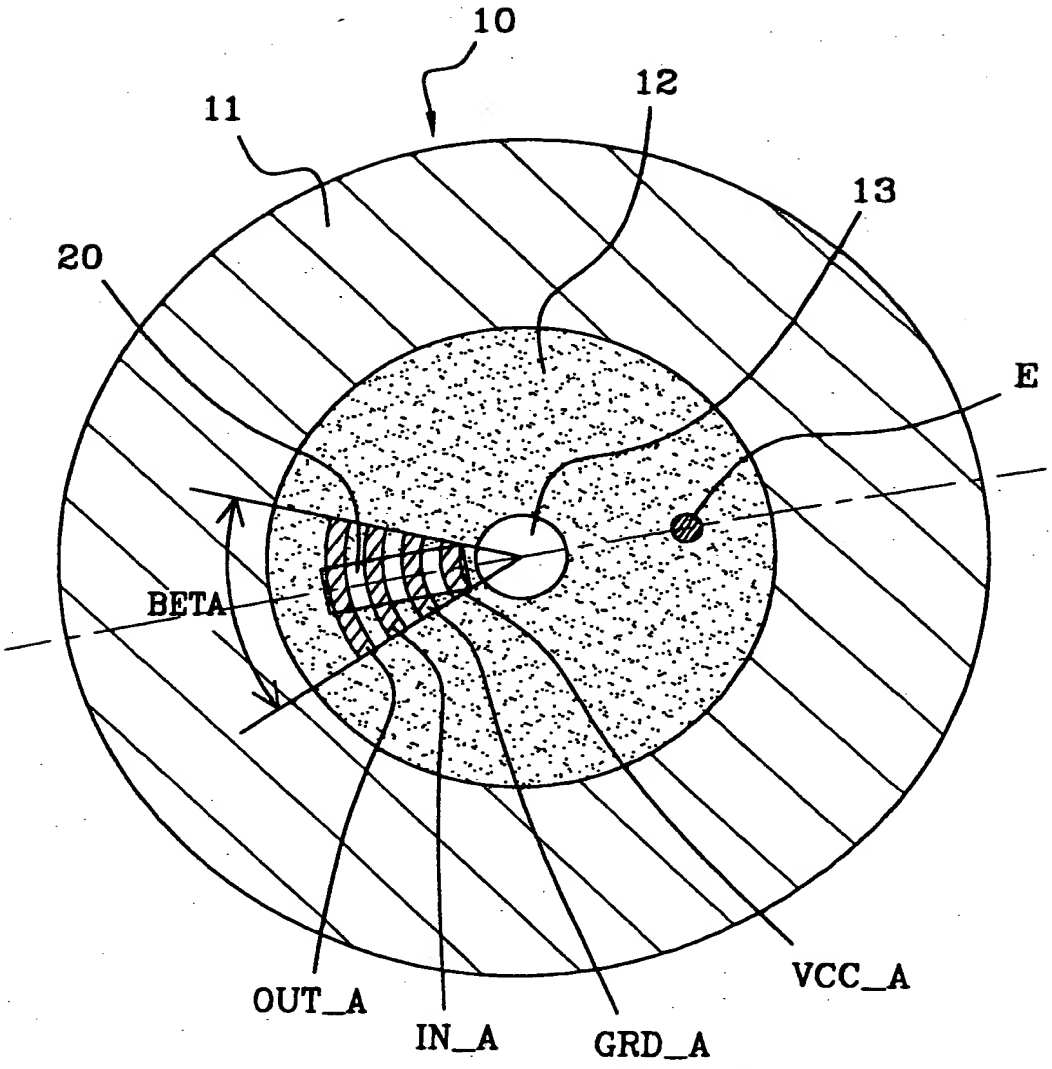

FIG.8

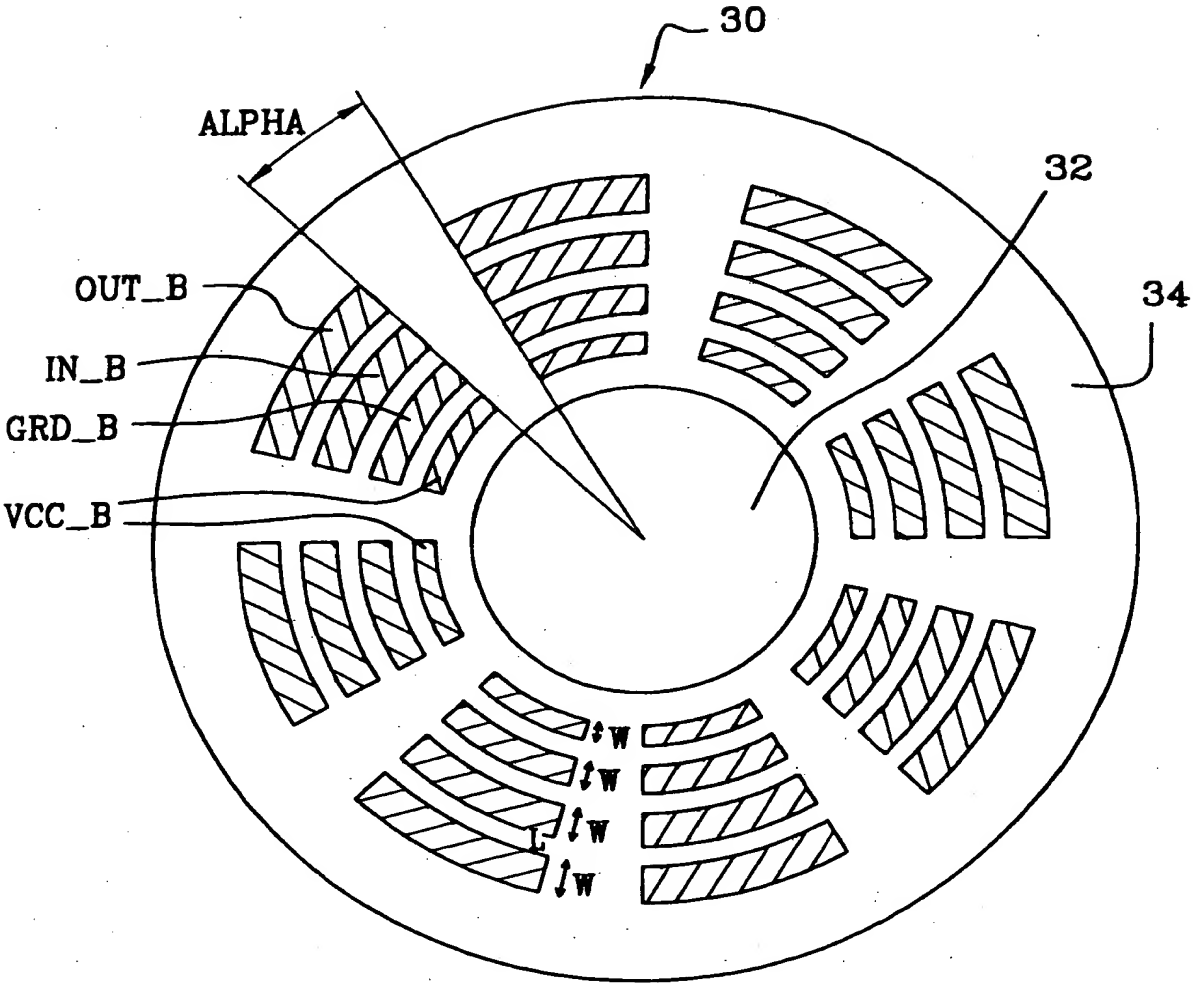

FIG.9

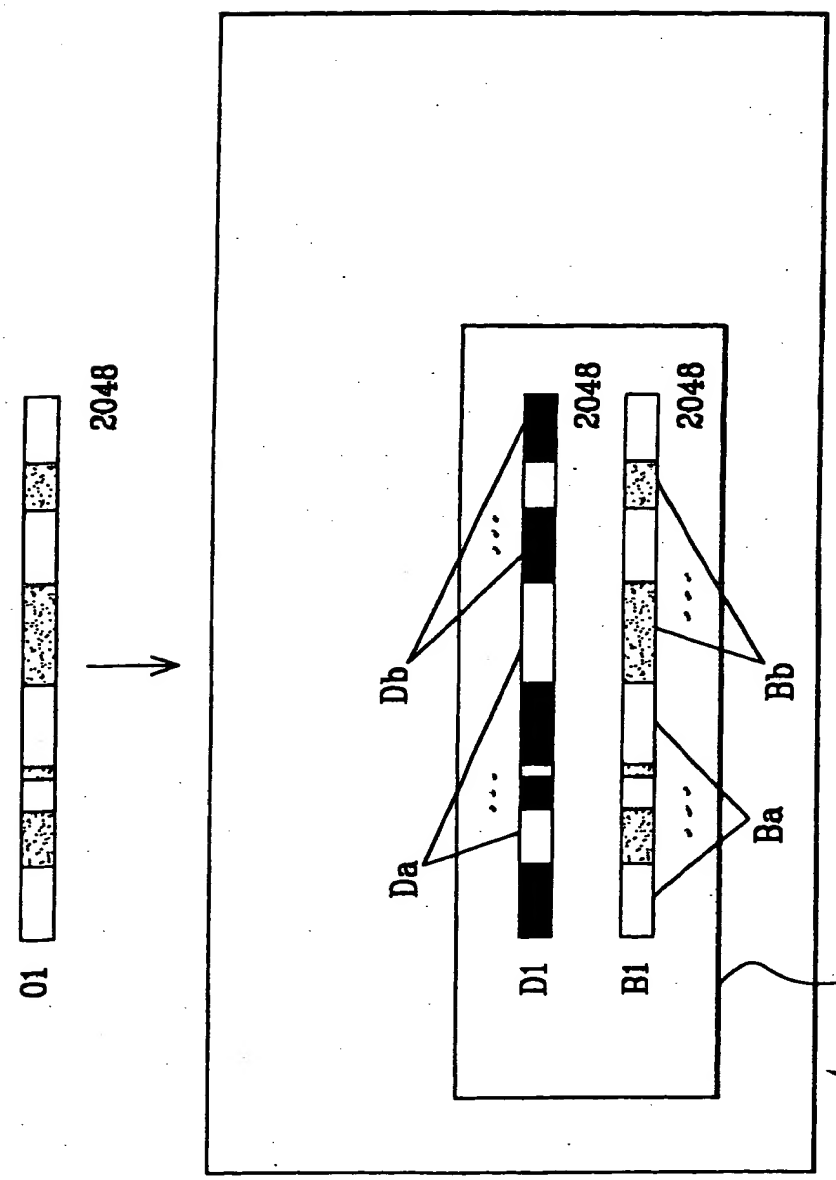

FIG.10

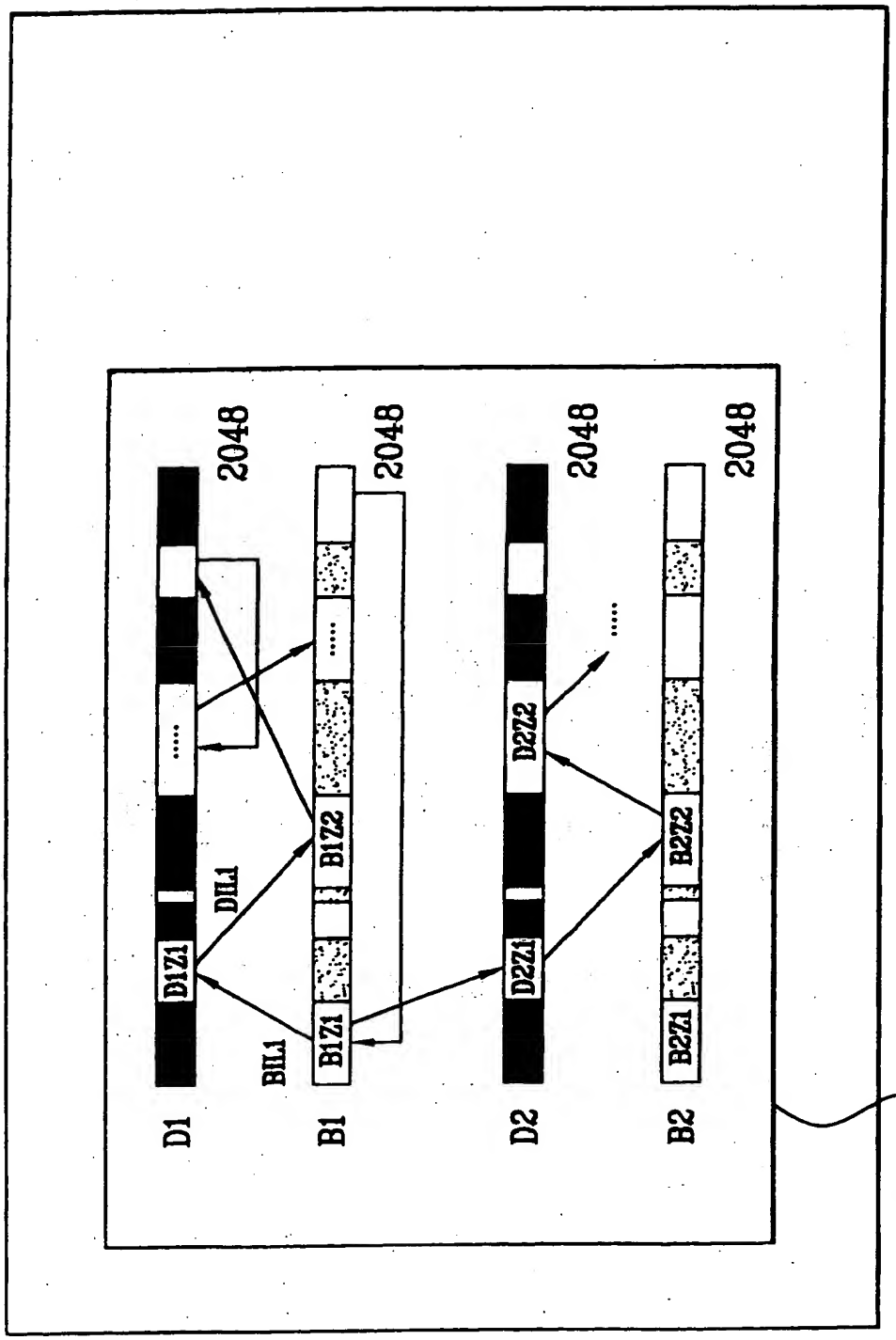
D1
B1
D2
B2
2048
2048
2048
2048
D1Z1
D1L1
B1L1
B1Z1
B1Z2
D2Z1
D2Z2
B2Z1
B2Z2
41
40

FIG.11

PROTECTED OPTICAL DISK AND METHOD FOR PROTECTING AN OPTICAL DISK.

The present invention concerns an optical disk for storing data. It also concerns a method for protecting said disk.

Applications of the invention can be particularly advantageous in fields such as data processing, games, audiovisual, etc. Data storage media, especially optical disks, include data intended to be generally exploited on a terminal, such as a computer or television monitor. Said data are either texts, images, sound or even software applications.

A large number of fraudulent copies of data contained in said media are made using software accessible to all users. These software applications are able to duplicate the data of a media despite copyright which generally protects said data. One known device of the prior art makes use of a security box to prevent pirate copies being made of the data contained in a media. The box, which contains an electronic identification circuit, is connected for example to a computer into which said media is introduced. Said device discloses the presence of a programme in the media making it possible to identify the security box by means of said electronic circuit. The programme is loaded into the computer and then carries out identification. In the absence of the appropriate box, the data cannot be read and accordingly the media cannot be used. The device only offers minimum security to the extent that the verification programme can be neutralised on the computer and then there is no longer any protection. Moreover, a protection box is generally associated with a single media item. As a result, the management of

security becomes cumbersome and complex since a new protection box is required for any new media item.

Also one technical problem to be resolved by the object of the present invention is obtaining a protected data storage optical disk, as well as a method for rendering secure said disk making it possible to avoid fraudulent copies being made of the data contained in said disks whilst not burdening the use of said disks.

According to a first object of the present invention, one solution to the technical problem stated as above is characterised in that said protected optical data storage disk comprises firstly a portable object comprising a memory including at least one secret key, and secondly data exchange means, said key being able to decrypt the data for said disk whilst remaining inside said portable object, said exchange means making it possible to exchange said data between said portable object and said disk.

According to the present invention, a method for protecting an optical disk is notable in that the method comprises the following stages consisting of :

- decrypting the data of said disk by means of a secret key included in a memory of a portable object integrated in said disk and remaining inside said object during decrypting,
- exchanging the data of said disk between said portable object and said disk by means of data exchange means integrated in said disk.

Thus, as shall be seen later in more detail, the device of the invention makes it possible to protect the data of the media by encrypting it and thus preventing a reading in uncoded form of said data. A copy of the data cannot be used as said data is encrypted. So as to read said data, the latter need to be

previously decrypted by means of a secret key included in said object integrated in the data storage media. Preferably, the secret key is unique to one media item. Thus, a reading of data in uncoded form is only possible from said media.

The following description with regard to the accompanying drawings, given by way of non-restrictive examples, shall clearly explain of what the invention consists of and how it can be embodied.

Figure 1 is a top view of a storage media conforming to the invention.

Figure 2 is a diagram of a portable object included in the media of figure 1.

Figure 3 is a side view of a media reader and the media of figure 1.

Figure 4 is a logic diagram of the media reader of figure 3.

Figure 5 is another logic diagram of the media reader of figure 3.

Figure 6 is a partial perspective view of the media reader of figure 3.

Figure 7 is a top view of a first embodiment of the media of figure 1.

Figure 8 is a top view of a second embodiment of the media of figure 1.

Figure 9 is a partial top view of the media reader of figure 3.

Figure 10 is a diagram of the data originating from the media of figure 1.

Figure 11 is another diagram of the data originating from the media of figure 1.

Figure 1 shows a data storage media 10. Said media integrates a portable object 20 and data exchange means. Said media 10 comprises three main zones. The peripheral zone 11 is able to store data. The other two zones are

central zones. One is a hole 13 placed at the centre of the media and in which a mechanical pin is able to slide, said zone thus corresponding to an axis of rotation. The other is a neutral zone 12 placed between the hole 13 and the peripheral zone 11 and contains no data. Said portable object 20 is integrated in a central zone of said media 10 which is the neutral zone 12. As shown on figure 2, the portable object 20 includes a memory 22 and a contacts block 23 for establishing electric contacts with a terminal, for example. The memory 22 includes a secret key K1. This key is preferably single for each media, in other words is no duplicate is provided either in the media to which it belongs or in other media. Said portable object 20 includes a cryptoprocessor 21. Said portable object is an integrated circuit chip. A chip is protected.

Said media 10 is an optical disk. An optical disk is a disk composed of tracks comprising data. Said data includes an application software such as a video game software or software for exploiting data bases.

The rest of the present summary of the invention deals with the example of CD-ROMs. Nevertheless, the invention of course can be applied generally to any other optical disk.

In the case of a CD-ROM, the data of a track are formatted according to standards, such as those called Yellow Book and Green Book defined by Philips. The standards basically define two data formatting modes. According to a first mode called mode 1, the track comprises user data, header data and error detection data able to have two error detection levels.. According to a second mode called mode 2, the track comprises user data, header data and error detection data having a single error detection level. The header data includes a track number and start and end of track indicators. The user data includes the application software.

The media 10 has three major phases. A production

phase, a customisation etching phase and a use phase.

During the production phase, the media 10 is placed on a milling machine which makes a housing in which the portable object 20 is integrated. Said object is inserted and glued in the housing. However, the weight of said portable object can render said media 10 out of balance. So as to avoid this problem, said media 10 is provided with balancing means E for balancing said media by replacing its centre of gravity on its spin axis. One non-restrictive embodiment of said balancing means shall be effected with the aid of a balancing feeder composed of a metal washer glued into a milling made in said media, said feeder being diametrically opposite to said portable object 20 of the media 10, as shown on figure 1. The production phase is ended.

During the customisation etching phase, data is encrypted and written in the media 10. Encryption and writing, also called etching, are made using an etching machine. Said etching machine is mainly composed of the following elements :

- a probe provided with contacts allowing an exchange of data between a computer controlling said machine and the portable object 20 integrated in the media 10,
- a cryptoprocessor representing an encryption algorithm for encrypting the data to be etched,
- a secret key generating software,
- a software for loading secret keys into the portable object 20 of the media 10.

The customisation-etching phase occurs according to the following stages :

- an unrecorded media 10 is loaded,
- an individual set of secret keys is generated,
- the data to be encrypted is determined,
- the data is encrypted with the aid of a sole secret key K1,

- said encrypted data is written in said media 10, as well as non-encrypted data,
- the individual set of secret keys are loaded into the portable object 20 of the media 10.

The sole secret key K1 is derived from the generated individual set of keys. Said key K1 is either one of the keys from the set of keys or a combination of keys from said set. So as to have an optimised management of the keys and associated media, several keys or sets of keys may derive from a given key, for example when keys are diversified from a "master" key. Similarly, so as to facilitate media management, a given secret key could be used for a series of media able to be recognised for example by a series number.

It is possible to choose to encrypt all the data of the media or only one portion. A track comprises data blocks of two thousand and forty-eight octets. The data is encrypted by groups of eight octets if an encryption algorithm, such as the DES, is used. Other symmetrical encryption algorithms can be used. All the data is etched in the peripheral zone 11 of the media. Etching is effected using known methods, such as magneto-optical methods or laser colorant burn-off.

From now on, the media 10 can be used.

During the use phase, in one first stage the data found in the media 10 is read using a media reader 30. As shown on figures 3 and 4, the reader is basically composed of a plate 35 housing the media 10, a motor M for making the media rotate, a mechanical spindle 32 which slides into the hole 13 of the media 10, two plates 33 and 34 for keeping the media 10 stable when the reader is functioning, a laser reading head 31 comprising in particular a laser diode and photodetectors, the laser diode being able to obtain a laser beam, an IDE or SCSI standard interface 36 for connecting said reader 30 to a computer 40, and a cryptoprocessor interface 37 allowing dialogue with the cryptoprocessor 21 of the portable object 20. The plate 34 is known as a doll

and is integral with the spindle 32.

Reading is made optically with the laser beam and is defined in standards called the Blue Book published by Philips. It is carried out according to a method based on detecting the reflection of a laser beam on a track at one time reflecting and at another time absorbing, thus defining data appearing in the form of light. The laser beam is accordingly directed towards the photodetectors which are transducers allowing a conversion of the light into electric signals. Said electric signals are processed at a first level so as to eliminate any discordance errors during a data reading. The track is then reconstructed and then a second level corrector code is applied when the latter is formatted with the mode 1. As a result, said track is sent to the interface 36 of said media reader 30.

The media 10 and the media reader 30 contain no details enabling the encrypted data to be dissociated from the non-encrypted data of a track. This thus avoids a fraud being made which would consist of copying the indications relating to an encryption mode of the data contained in the media 10.

In a second stage, the media reader 30 recognises whether the media 10 is equipped with a cryptoprocessor. To this end, it sends the track read via its cryptoprocessor interface 37 to the media 10. In a case where data is sent back by said media via a first communication channel 361 open prior to reading of said media 10, said channel being included in the interface 36, the reader 30 shall conclude that a media 10 is present comprising a portable object 20 composed of a cryptoprocessor 21. In the opposite case, no data element is sent back and accordingly the media 10 contains no cryptoprocessor and data reading is made without decryption.

In a third stage in a case where the media 10 is equipped with a cryptoprocessor, as shown on figure 4, the read data DATA is sent to the computer 40 connected to said

reader 30 via a second communication channel 362 open prior to reading of said media 10, said channel being included in the interface 36. This data is known as unprocessed data as said data has not been modified. At the same time, the read data DATA is sent to the cryptoprocessor 21. According to a first embodiment, said data DATA is sent via the cryptoprocessor interface 37. Thus, before being sent to the cryptoprocessor, the data DATA is firstly modified into a format able to be understood by the cryptoprocessor, such as into octets, via the cryptoprocessor interface 37 included in the optical disk reader.

According to a second embodiment as shown on figure 5, said data DATA is sent to the cryptoprocessor 21 of the portable object 20 with the aid of an all-purpose series linking bus 38 known as a USB, said bus being integrated in the computer 40. Accordingly, a single communication channel included in the interface 36 of the reader 30 is required. The decrypted data in said cryptoprocessor 21 are then sent back to the computer 40 via this same bus 38. Here it is the computer 40 which comprises a cryptoprocessor interface which modifies the data DATA into a format able to be understood by the cryptoprocessor.

It shall be noted that this embodiment can also be used during the second stage described previously.

At the time the data DATA read is sent to the cryptoprocessor, the electric signals of the media reader 30 corresponding to said data are transferred to the media 10 and from the media 10 to the portable object 20 by means of data exchange means integrated in said media and via exchange means integrated in the media reader 30.

Either the data exchange means integrated in said media 10 have contacts or the data exchange means integrated in said media 10 have no contacts.

In the case of data exchange means with no contacts, according to a non-restrictive embodiment of the invention,

the data exchange means integrated in said media 10 have an antenna. The data exchange means integrated in the reader 30 have a second antenna. In this case, the data is exchanged via inductive coupling between said first and second antennae.

In the case of data exchange means with contacts, according to a first non-restrictive embodiment of the invention as shown on figure 6, first exchange means IN_B, OUT_B, VCC_B and GRD_B are integrated in the media reader 30 at the level of the spindle 32 and the doll 34, and as shown on figure 7 the data exchange means IN_A, OUT_A, VCC_A and GRD_A are integrated in the media 10 at the level of a central zone which is the neutral zone 12. When the doll 34 is in contact with the media 10, the first means enter into contact respectively with the second means. This makes it possible to exchange data between said media reader and said media. In addition, the second means IN_A, OUT_A, VCC_A and GRD_A integrated in the media 10 are connected to the contact block 23 of the portable object ar respective contact points I, O, V and G. Said second means IN_A, OUT_AZ, VCC_A and GRD_A also allow an exchange of data between said media 10 and said portable object 20. Thus, said data exchange means integrated in the media 10 and the reader 30 include input exchange means IN_A, IN_B, output exchange means OUT_A, OUT_B, feed means VCC_A, VCC_B and earthing means GRD_A, GRD_B.

The input exchange means IN_A and IN_B make it possible to transport the data from the media reader via the media 10. The contact point 1 and the input device IN_A make it possible to send the data of the media 10 to the portable object 20. The output exchange means OUT_A and OUT_B make it possible to transport data from the media 10 via the media reader 30. The contact point O and the output device OUT_A make it possible to transmit the data from the portable object 20 to the media 10. The feed means VCC_A and VCC_B

feed said portable object 20 with voltage and the earthing means GRD_A and GRD_B enable said portable object to be earthed.

According to a second embodiment, the data input exchange means IN_A, IN_B and the data output exchange means OUT_A, OUT_B can be merged and thus be bidirectional exchange means.

It shall be noted that according to another embodiment, the first data exchange means IN_B, OUT_B, VCC_B and GRD_B integrated with the media reader 30 can be integrated at the level of the lower plate 33 of the reader.

So as to allow an effective transport of the electric signals, said data exchange means integrated in said media 10 are composed on a material allowing good conductivity and avoiding excessive oxidation of said means. Thus they are made of gold. For example, said means can be rings as shown on figure 7, wires or even arcs of circles as shown on figure 8. The same applies to the data exchange means integrated in the media reader 30. So as to avoid the presence of a loop sensitive to the electromagnetic radiation and thus avoid radio interference due to this radiation, the data exchange means integrated in said media 10 are arcs of circles forming a circular sector with a BETA angle and the data exchange means of the reader 30 are circle arcs spaced by an ALPHA angle smaller than the BETA angle, as shown on figure 9. The arcs of circles of the media 10 and the reader 30 have the same width W and are distant from a given width L. Thus, permanent contact is guaranteed between the various data exchange means.

After the electric signals corresponding to the read data DATA are sent to the portable object 20 by means of the previously defined data exchange means, the data is decrypted with the aid of a cryptoprocessor using the sole secret key K1 included in the memory 22 of the portable object 20. By means of this sole key system integrated in a

portable object, a copy of the data of the media 10 on a second media, possibly comprising a cryptoprocessor, cannot be used.

Said cryptoprocessor represents an algorithm opposite the one used to encrypt said data. Said cryptoprocessor is programmed or wired.

According to a first non-restrictive embodiment, said cryptoprocessor is integrated in said portable object 20. The secret key K1 does not come out of the chip but stays there. According to a second embodiment, the cryptoprocessor is a cryptoprocessor attached to the media reader 30. In this second embodiment, the secret key K1 of the portable object 20 needs to be sent into the reader temporarily, namely the time to decrypt the read data DATA. It is clear that in this case there is no need to send the data DATA to the portable object 20. However, the first embodiment would be preferred, said embodiment offering far more protection given the fact that the secret key K1 remains in the portable object 20 and never transmitted outside and is thus not subject to frauds which would consist of spying on the media reader 30 so as to reconstruct said secret key K1. Moreover, the fact that the cryptoprocessor is in the portable object prevents a fraudulent person copying the means allowing encrypting or decrypting.

In the cryptoprocessor, the data DATA is decrypted systematically whether said data has been originally encrypted or not, and then if appropriate, are sent back to said reader 30 and finally sent to the computer 40 via the first communication channel 361 if the crytoprocessor interface 37 is used.

Alternatively, the unprocessed and decrypted data DATA of said media 10 is loaded into a memory 41 of the computer 40. The computer could therefore mark the various sent sets of data. As shown on figure 10, the unprocessed B and decrypted D data is sent to the computer 40 preferably by

tracks or complete blocks or octets. It shall be noted that the data, not originally encrypted but decrypted via the cryptoprocessor 21, are not useable. However, the fact that the reader 30 systematically sends the computer 40 the unprocessed and decrypted data makes it possible to be forewarned of an attack which would firstly consist of differentiating the encrypted and non-encrypted data, and secondly find a way to use them by quite simply being connected to the outlet of the media reader 30.

In a fourth stage, the data sent and loaded into the memory 41 of the computer 40 is used as follows : said data, which includes the application software of the media 10, is composed of a pair of tracks or blocks, one track or block B1 being unprocessed and one track or block D1 being decrypted whose origin is a track or block O1 of data read in the media 10. Figure 10 shows an unprocessed block B1 composed firstly of zones Ba of non-encrypted data known as useful zones, and secondly zones Db of decrypted unusable data unable and zones Da, also known as useful zones, of decrypted data corresponding to the zones Bd of encrypted data of the unprocessed block B1.

The application software firstly includes a self-starting programme recognised by the computer making it possible to initialise said software, and secondly the executable code. Said executable code includes a set of links for interconnecting various zones and load new data into the memory and reconstruct a data zone. Said start-up programme is initially loaded into the computer 40.

The useful zones of the various blocks generally comprise firstly a portion of the executable code, and secondly application data used by the application software, such as images, text, sound.

As shown on figure 11, the unprocessed block B1 comprises a first useful zone B1Z1 whose executable code is executed and uses the application data required for said

execution. At the end of execution of said code, a first link B1L1 is positioned on a first useful zone D1Z1 of the decrypted block D1. The code of said zone is executed. At the end of execution said code, a link D1L1 of said zone D1Z1 is positioned on a second useful zone B1Z2 of the unprocessed block B1 whose code is executed, and so on. When the final useful zone of the unprocessed block B1 is executed, a link makes it possible to load into the memory 41 of the computer the blocks or tracks of data required by the application software. Thus, one or several other pairs of unprocessed and decrypted tracks or blocks are read and loaded into the memory 41. Thus, according to the foregoing, it shall be extremely difficult for a person intent on fraud to reconstruct the executable code.

It shall be noted that, according to the optical disk 10 of the invention including a cryptoprocessor as previously described, the reader 30 could include a decryption service. Thus, data shall be sent from the computer 40 to the cryptoprocessor 21 of the media 10 so as to decrypt said data. This service shall be useful for certain security architectures in which the application software would have to decrypt track portions during execution of said software.

The invention described above has other advantages described hereafter. The invention has the advantage of firstly being able to protect applications written in a high level language, and secondly allow management of a large number of applications. To this end, the optical disk 10 comprises DATA forming at least one application written in high level language, especially in JAVA language (registered trademark). Said applications are preferably fully or partially encrypted. Thus, said applications are protected as described previously and could not be duplicated. Moreover, as the optical disk has a large memory capacity, it would be possible to manage a large number of

applications. Thus, an applications supplier will be able to promote its applications and distribute them in bulk. Advantageously, the optical disk is accessible on writing/reading for an applications supplier. As a result, the supplier could itself manage the applications on the optical disk at any time. For example, at a point of sale, the supplier could download applications into a disk from one of its computers or servers.

The optical disk of the invention could be of interest in the field of mobile telephones. A mobile telephone comprises a telephone smart card currently known as an SIM card. According to a known prior art, when a user of the mobile telephone wishes to use a service of an operator, either the application relating to said service is found on his mobile telephone or needs to be downloaded into the SIM card from a server of the operator via a network managed by said operator. Often the operators offers new services, such as a banking telephone service, to users whose applications need to be downloaded. The applications are generally written in JAVA language so as to be able to be modified and managed by the operator. Downloading is a long process, less reliable and the network is often congested. In addition, the SIM card has a reduced memory and cannot support all the applications offered by the operator. By means of the optical disk of the invention, an operator can distribute its applications to users already protected and avoids its network becoming congested and the memory of the SIM card becoming overloaded. The user buys an optical disk comprising the applications relating to the services he needs. Thus, he merely needs to insert the optical disk into his computer and his SIM card into a card reader connected to his computer and select the application he wants to load into his card. It may be desired to have the optical disk only being accessible on reading by the user so as to prevent him from modifying certain data of the applications.

CLAIMS

1. Protected optical disk (10) for storing data, characterised in that it comprises firstly a portable object (20) comprising a memory (22) including at least one secret key (K1), and secondly data exchange means, said key (K1) able to decrypt the data (DATA) of said disk whilst remaining inside said portable object (20), said exchange means (IN_A, OUT_A, VCC_A, GRD_A) making it possible to exchange said data between said portable object and said disk.

2. Optical disk according to claim 1, characterised in that said portable object is a chip with an integrated circuit.

3. Optical disk according to one of the preceding claims, characterised in that said portable object is integrated in a central zone of said disk (10).

4. Optical disk according to one of the preceding claims, characterised in that the data exchange means (IN_A, OUT_A, VCC_A, GRD_A) are integrated in a central zone of the disk (10).

5. Optical disk according to one of the preceding claims, characterised in that it comprises balancing means (E) for balancing said disk.

6. Optical disk according to one of the preceding claims, characterised in that the data exchange means integrated in said disk (10) have contacts.

7. Optical disk according to one of claims 1 to 5, characterised in that the data exchange means integrated in said disk (10) have no contacts.

8. Optical disk according to one of the preceding claims, characterised in that the data (DATA) is decrypted using a cryptoprocessor.

9. Optical disk according to claim 8, characterised in that said cryptoprocessor is integrated in said portable

object (20).

10. Optical disk according to claim 8, characterised in that the data (DATA) is firstly modified into a format able to be understood by the cryptoprocessor by means of a cryptoprocessor interface (37) included in an optical disk reader.

11. Optical disk according to claim 8, characterised in that the data (DATA) is firstly modified into a format able to be understood by the cryptoprocessor by means of a cryptoprocessor included in a computer (40).

12. Optical disk according to one of claims 1 to 11, characterised in that data (DATA) from the disk is intended to be systematically decrypted whether said data has been originally encrypted or not.

13. Optical disk according to one of claims 1 to 12, characterised in that a set of unprocessed data (B) and a set of decrypted data both sets originating from a set of data read in the disk (10) are intended to be sent to a computer (40).

14. Optical disk according to claim 13, characterised in that a set of unprocessed data (B) is composed of at least one zone of unusable encrypted data and a set of decrypted data (D) is composed of at least one zone of usable decrypted data (Da).

15. Optical disk according to claim 14 or 15, characterised in that a set of unprocessed data (B) is composed of at least one zone of usable non-encrypted data (Ba) and a set of decrypted data (D) is composed of at last one zone of unusable decrypted data (Dd).

16. Optical disk according to claim 13 or 14, characterised in that a useful data zone comprises an executable code portion and application data.

17. Optical disk according to claim 16, characterised in that the executable code includes a set of links for interconnecting various data zones, load new data into the

memory and reconstructing a data zone.

18. Optical disk according to one of claims 1 to 17, characterised in that the data (DATA) of the disk form at least one application written in high-level language.

19. Optical disk according to claim 18, characterised in that the application is partially or totally encrypted.

20. Method for protecting an optical disk (10) for storing data, characterised in that the method comprises stages according to which :

- data (DATA) of said disk (10) is decrypted with the aid of a secret key (K1) included in a memory (22) of a portable object (20) integrated in said disk and remaining inside said object during decryption,
- the data (DATA) of said disk (10) is exchanged between said portable object (20) and said disk by means of data exchange means (IN_A, OUT_A, VCC_A, GRD_A) integrated in said disk.

21. Method according to claim 20, characterised in that said portable object is a chip with an integrated circuit.

22. Method according to claim 20 or 21, characterised in that the decryption stage is carried out using a cryptoprocessor integrated in said portable object (20).

23. Method according to claim 22, characterised in that it comprises an additional stage according to which :

- prior to the decryption stage, the data (DATA) is modified into a format able to be understood by the cryptoprocessor via a cryptoprocessor (37) included in an optical disk reader.

24. Method according to claim 22, characterised in that it comprises an additional stage according to which :

- prior to the decryption stage, the data (DATA) is modified into a format able to be understood by the cryptoprocessor by means of a cryptoprocessor interface (37) included in a computer (40).

25. Method according to one of claims 20to 24,

characterised in that in the decryption stage the data (DATA) is decrypted systematically regardless of whether said data was originally encrypted or not.

26. Method according to one of claims 20 to 25, characterised in that it comprises an additional stage according to which :

- a set of unprocessed decrypted data (D) originating from a set of data read in the disk (10) is loaded into a computer (40).

27. Method according to claim 26, characterised in that loading is carried out alternately.

28. Method according to claim 26, characterised in that a set of unprocessed data (B) is composed of at least one zone of unusable encrypted data (Bb) and a set of decrypted data (D) is composed of at least one zone of usable decrypted data (Da).

29. Method according to claim 26, characterised in that a set of unprocessed data (B) is composed of at least one non-encrypted useful zone of data (Ba), and a set of decrypted data (D) is composed of at least one zone of unusable decrypted data (Dd).

30. Method according to claim 28 or 29, characterised in that it comprises an additional stage according to which :

- one executable code portion included in the useful data zone is executed including application data.

31. Method according to claim 30, characterised in that it comprises an additional stage according to which :

- various data zones are interconnected, new data is loaded into the memory and a data zone is reconstructed with the aid of a set of links included in the executable code.

32. Method according to one of claims 20 to 31, characterised in that it comprises an additional stage according to which :

- data is encrypted by means of a secret key (K1),
- said encrypted data is written in said disk (10).

33. Method according to one of claims 20 to 32, characterised in that it comprises data (DATA) forming at least one application written in high-level language.

34. Method according to claim 33, characterised in that the application is partially or totally encrypted.

ABSTRACT TO THE DISCLOSURE

The invention concerns a protected optical disk for storing data. It also concerns a method for protecting said disk. The invention is characterised in that said disk firstly comprises a portable object comprising a memory including at least one secret key, and secondly data exchange means, said key making it possible to decrypt the data of said disk whilst remaining in said portable object, said exchange means making it possible to exchange said data between said portable object and said disk. The invention can be applied in particular to CD-ROMs.

Figure 8